Abstract

A method and system are configured for synchronous broadcast communications by applying signature keys using hashing functions. Each subsequent transmission in a sequence includes a signature key that can be verified by hashing to a preceding signature key from a previous portion of the sequence. The first transmission in the sequence is signed using a signature key that is known by the client device, typically verified using some other mechanism such as asymmetric key signatures. Each client device can utilize an internal counter for the current time or the block number in the transmission sequence to maintain synchronized transmissions in the even that a particular portion of the sequence is missed, and to validate signature keys. Since the signature keys can be validated when they are received but not predicted before they are received, the transmission is difficult to attack while synchronization is maintained.